Setting the Standard for Automation™

Industrial Cybersecurity Training Coming to Alabama!

Using the ANSI/ISA-62443 Standards to Secure Your Industrial Control System (IC32)

The move to using open standards such as Ethernet, TCP/IP, and web technologies in supervisory control and data acquisition (SCADA) and process control networks has begun to expose these systems to the same cyberattacks that have wreaked so much havoc on corporate information systems. This course provides a detailed look at how the ANSI/ISA99 standards can be used to protect your critical control systems. It also explores the procedural and technical differences between the security for traditional IT environments and those solutions appropriate for SCADA or plant floor environments.

This course is required for the ISA99/IEC 62443 Cybersecurity Fundamentals Specialist Certificate Program.

You will be able to:

- Discuss the principles behind creating an effective long term program security
- Interpret the ANSI/ISA99 industrial security guidelines and apply them to your operation
- Define the basics of risk and vulnerability analysis methodologies
- Describe the principles of security policy development
- Explain the concepts of defense in depth and zone/conduit models of security
- Analyze the current trends in industrial security incidents and methods hackers use to attack a system
- Define the principles behind the key risk mitigation techniques, including anti-virus and patch management, firewalls, and virtual private networks

You will cover:

- **Understanding the Current Industrial Security Environment:** What is Electronic Security for Industrial Automation and Control Systems? | How IT and the Plant Floor are Different and How They are the Same
- **How Cyberattacks Happen:** Understanding the Threat Sources | The Steps to Successful Cyberattacks
- **Creating A Security Program:** Critical Factors for Success/Understanding the ANSI/ISA-62443-2-1 (ANSI/ISA-99.02.01-2009) *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*
- **Risk Analysis:** Business Rationale | Risk Identification, Classification, and Assessment | The DNSAM Methodology
- **Addressing Risk with Security Policy, Organization, and Awareness:** CSMS Scope | Organizational Security | Staff Training and Security Awareness
- **Addressing Risk with Selected Security Counter Measures:** Personnel Security | Physical and Environmental Security | Network Segmentation | Access Control
- **Addressing Risk with Implementation Measures:** Risk Management and Implementation | System Development and Maintenance | Information and Document Management
- **Monitoring and Improving the CSMS:** Compliance and Review | Improve and Maintain the CSMS

Classroom/Laboratory Exercises:

- Develop a business case for industrial security
- Conduct security threat analysis
- Investigate scanning and protocol analysis tools
- Apply basic security analysis tools software

Includes ISA Standards:

- ANSI/ISA-62443-1-1 (ANSI/ISA-99.00.01-2007) *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts & Models*
- ANSI/ISA-62443-2-1 (ANSI/ISA-99.02.01-2009) *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*
- ANSI/ISA-62443-3-3—*Security for industrial automation and control systems: System security requirements and security levels*

More ➤

To register for this comprehensive course, visit **www.isa.org/2015/BHAMIC32** or call **+1 919-549-8411**.

Early Bird Discount and Deadline!

Save 5% when you register for this course offering by **2 April 2015** using Promo Code: **IC3215BHAM**

IC32 Quick Quiz

1. **Which three basic properties are the building blocks of cyber security?**
   a. Authorization, Identification, and Integrity (A I I)
   b. Availability, Integrity, and Confidentiality (A I C)
   c. Authorization, Reliability, and Integrity (A R I)
   d. None of the above

2. **What is the biggest security problem if business networks connect directly to industrial control systems?**
   a. Too many business users requesting data will slow control system operation to a crawl, endangering the security of processes.
   b. Unauthorized business users, outsiders and malware can penetrate critical industrial control systems and upset critical processes.
   c. Production workers will change data in business systems given the opportunity.

3. **"Countermeasures" in cyber security are measures taken to:**
   a. Eliminate system penetration by outsiders
   b. Confuse perimeter intrusion detectors
   c. Reduce the system's risk of loss from vulnerabilities and threats
   d. Eliminate the risk of an inside attacker taking over a computer network

Learn the answers to these critical questions AND find out more about the requirements of the ANSI/ISA-62443 industry standards by attending this informative course today.

Your Instructor

Bryan L. Singer CISM, CISSP, CAP has over 15 years' experience in information technology security—including 7 years specializing in industrial automation and control systems security, critical infrastructure protection, and counter-terrorism. His background focuses on software development, network design, information security, and industrial security. His industry experience includes healthcare, telecommunications, water/wastewater, automotive, food and beverage, pharmaceuticals, fossil and hydro power generation, and oil and gas industries.

Mr. Singer has specialized in process intelligence and manufacturing disciplines such as historians, industrial networking, Power and Energy Management (PEMS), Manufacturing Enterprise Systems (MES), Laboratory Information Management Systems (LIMS), Enterprise Resource Planning (ERP), and Condition Based Monitoring (CBM). He began his professional career with the US Army as an Intelligence Analyst. After the military, he worked in various critical infrastructure fields in software development and systems design, including security.

Mr. Singer has worked for various companies such as EnteGreat, Rockwell Automation, FluidIQs, and Wurldtech, before joining Kenexis Consulting, and co-founding Kenexis Security in 2008. At Kenexis, he is responsible for development, deployment, and management of industrial network design and security services from both a safety and system architecture perspective. He also served as the co-chairman of ISA99 Security Standard, and a former board member of the Department of Homeland Security's Process Control Systems.

Course Details

Date: ..... 30 April – 1 May 2015
Time: ..... 8:00 a.m.–4:00 p.m.
Location: ..... UAB Engineering Complex
BEC 158
1150 Tenth Avenue South
Birmingham, AL 35294
Course No.: IC32
CEU/PDH Credits: 1.4/14
Registration: ..... Member: $1,265; Non-member: $1,585
Group: $1,265; Affiliate: $1,425
Community Member: $1,585

- **The Early Bird Discount Deadline is 2 April 2015.**
- **The last day to pre-register online is 16 April 2015.**

To register, call +1 919-549-8411 or visit www.isa.org/2015/BHAMIC32.

Space is Limited—Register Now!

Event Contributors:

Alabama Technology Network
ISO 9001:2008

UAB IEM
INFORMATION ENGINEERING & MANAGEMENT

How can you SAVE on ISA Training?
Become an ISA member.

Learn more about the benefits of ISA membership—including ISA member rates, a discount of 20% on training—at **www.isa.org/MemberPrice**.